user having previously performed a first run of that same authentication procedure in order set up a connection, e.g., a GPRS connection. The second authentication run, i.e., an authentication re-run, results in security data which the authentication node transfers to the forwarding agent using the trusted relationship between these two entities. In effect, the user has authenticated to the forwarding agent, and thus, the forwarding agent can trust that a public key received from the user really belongs to the user as, e.g., identified from subscriber data received from the network/authentication node. Thus, the forwarding agent, representing the other separated system, may update the subscriber database and DNS server with linked data: subscriber identity/FQDN/IP/public key.

The claims explicitly recite first and second runs of the same authentication method related to the cellular system for the same mobile node, which is the basis for updating a home agent with a current address in the cellular system. User identity is bound with a public key such that any other user, knowing the IP-address of the user, may establish a secure communication with the user being certain that the public key really belongs to the alleged user. This corresponds to a certification of the public key.

The Examiner's rejection, although set out at great length, boils down to the following: the Examiner believes that Haverinen discloses all of the features of claims 23 and 30 except for updating a subscriber database and DMS server with a FQDN and/or IP address, and that this feature is taught by Ju. Applicants respectfully disagree.

Haverinen describes a second authentication between a MT and a visited network (FAAA) (presumably being mapped by the Examiner to the claimed stable forwarding agent) in addition to a first authentication already established between the MT and its a home network (HAAA) (presumably being mapped by the Examiner to the claimed radio communication network). The second authentication is described in paragraphs 0177 to 0187. There is no teaching or suggestion in Haverinen that this second authentication process binds a user identity to a public key or uses subscriber data to form a FQDN which is then stored.

The following steps in claim 23 are not disclosed in Haverinen:

1. sending a public key from the mobile node to the stable forwarding agent;

2. following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from the authentication server;

3. using the subscriber contact information to assign a FQDN and/or IP address to the mobile node; and

4. updating a subscriber database and DNS server with the FQDN and/or IP address and the public key provided by the mobile node.

For the step labeled above as (1) of sending a public key from the mobile node to the stable forwarding agent, the Examiner points to paragraph 183 of Haverinen describing computing cryptographic checksum SIGNsres, which is then sent to the HAAA via FAAA. The Examiner equates the cryptographic checksum SIGNsres to the public key of the mobile node. The rejection then refers to the mobile terminal using a public key (K) "in" the checksum SIGNsres "to encrypt the IMSI value sent over in the IDmt pay load." First, the public K is described in paragraph 183 as being used to test SIGNrand rather than being "in" " the checksum SIGNsres. Second, SIGNsres is a checksum and not a key. It certainly is not the public key K. The fact that the shared secret K is later used for encryption and not SIGNsres confirms this.

Throughout Haverinen, the "signatures" (SIGNrand, SIGNsres, SIGNresult, and SIGN_SRES) are keyed hashes. They are not public key signatures, but used to generate signatures in a protocol based on shared secrets. Thus, there is no teaching or suggestion in Haverinen of the claimed sending a public key from the mobile node to the stable forwarding agent.

Labeled step (2): following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from the authentication server is also missing from Haverinen. The Examiner points to paragraphs 0187 and 0188 in Haverinen as teaching this claim feature. Paragraph 0187 is the last step (step 10) in Haverinen's FAAA-MT authentication procedure where authentication is complete with the visited network (FAAA) and mobile node (MT) both having access to a shared secret K.

It is important to understand that paragraph 0188 does not refer to a process carried out after this step 10 in Haverinen, as the office action suggests. Rather, paragraph 0188 describes how the FAAA selects a suitable home authentication server (HAAA) to run the authentication procedure. In other words, paragraph 0188 provides more details as to how the FAAA selects a HAAA for use in steps and 1 and 2 (paragraphs 0178 and 0179 in Haverinen). Paragraph 0188 is not a procedure performed following authentication of the mobile node to the stable forwarding agent (FAAA).

There is also no suggestion of collecting at the stable forwarding agent (FAAA) subscriber contact information from the authentication server (HAAA). Paragraph 0188 is concerned only with selection of the authentication server (HAAA) using the domain part of the user's NAI provided by the mobile terminal MT. There is no teaching or suggestion of collecting any information from the authentication server HAAA, and in particular, no teaching or suggestion of collecting subscriber contact information. This paragraph only describes using subscriber contact information to select the HAAA.

Haverinen further lacks the claim feature of using the subscriber contact information to assign a FQDN and/or IP address to the mobile terminal. The Examiner relies on paragraph 0165 which defines the NAI of the mobile terminal to include a domain part. The Examiner alleges that paragraph 0188 refers to the assignment of the FQDN and/or IP address to the mobile terminal. But, as just explained, paragraph 0188 refers to the selection of the HAAA on the basis of the NAI domain part provided by the mobile terminal. There is no disclosure of assigning an FQDN and/or IP address. Nor is there a teaching of assigning anything based on subscriber contact information collected from the authentication server HAAA.

If Haverinen makes a hint about assigning the IP address, it is assigned by a DHCP server. Indeed, the main idea of Haverinen is that the mobile node does not need to change its IP address. In contrast, the claims describe the mobile node getting a new IP address which is then stored into the DNS and subscriber database.

The Examiner acknowledges that Haverinen does not teach updating a subscriber database and DNS server with the FQDN and/or IP address and the public key provided by the mobile node. For this feature, the Examiner alleges that it would be obvious to use the IP address allocation and storage described in paragraph 13 of Ju. However, Ju does not describe updating a subscriber database with any information, and nor does it describe including a public key in any update of a subscriber database or DNS server. The point of this last claim step is to bind together the authentication of the mobile node with the subscriber contact details to ensure that the authentication can be used for provision of further mobile services. There is no suggestion of this in either Haverinen or Ju. Moreover, Haverinen strives for IP-level stability where the mobile terminal's IP address does not change. The claimed technology, on the other hand, is concerned with IP mobility where the mobile terminal's IP address does change.

Since the combination of Haverinen and Ju lack multiple features recited in the independent claims, the rejection should be withdrawn. Accordingly, the application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100